

The following is a compilation of the questions and answers from the NESNIPPRIVACY Work Group listing.

Questions about consents and authorizations:

Question: We had a request from the mother of a deceased individual for release of her deceased daughter's records specifically to ascertain if she had, in fact, had a miscarriage prior to the birth of her only child. The woman was divorced, so we are assuming we have to release the records to the next-of-kin mother, as the woman's only child is still a minor. Are any legal documents required giving her authorization to obtain this information? Does she have a valid "need to know?"

Answer: I am including language from our Release of Information policy. The HIPAA regulations will not significantly change how we deal with records of decedents. We ask for an authorization from the executor or administrator of the decedent's estate.

"In the event a patient or former patient dies and a personal representative or administrator is appointed, only the personal representative and/or administrator of the patient's estate, and not the spouse, may authorize release of information."

In the situation above, you should copy the document from the probate court appointing the individual as executor/administrator. If no appointment has been made, you can release the documents to next of kin with a signed authorization

The HIPAA provision regarding disclosures for deceased individuals states:

"If under applicable law an executor, administrator, or other individual has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter with respect to protected health information relevant to such personal representative."

Question: We had a situation recently where a 23-year-old patient was provided with health services at our facility. Legally, he is an adult and can give consent for himself, but he is still covered under his parents' health insurance policy while he is in college. Rather irate, this patient's father contacted our facility to receive information about his child's care, but our staff declined to release this confidential information, but did say that the information could be released if consent was given by his son. Does this parent have the right to obtain his adult child's medical record information, without patient consent, if the parent is still insuring the child? Where are the HIPAA boundaries? (We wanted to act conservatively and be sure that we had the correct answer before releasing the info.)

In another similar scenario, a married woman (who is insured under her husband's policy) receives health care at our facility. Can her husband obtain access to her medical records without permission/consent by his wife? Or, does the fact that he is the policy holder and

the one to give consent to treat should his wife be unable, give him the right to access her health records?

Answer: 1. It does not matter if the adult child (age 19 or older in NE) is covered under the parents' insurance. It is still his medical information and he should give authorization for its release. Mom and Dad do not have the right to read their son's chart, even though they may be paying for the treatment. The insurance /payment issues are entirely separate from the disclosure issues. The only exception to this rule is if an adult child has been deemed incompetent by a court and the parents are appointed legal guardians. Then they can have full access.

Likewise, a spouse should not be giving authorization if the patient is competent. If the patient is not capable of giving consent, then you should look for a durable power of attorney paper, if it exists.

(Nancy Kinyoun, Health Information Manager, Hastings Regional Center, Hastings, NE)

2. I generally agree with Nancy's response. I recommend also reviewing 164.510(b) - Uses and Disclosures for Involvement in the Individual's Care and Notification. There are limited disclosures that can be made to family members under specific circumstances. (Ron Hoffman, Corporate Privacy Team, Mutual of Omaha)

Question: I've been thinking back to the recently implemented MQRSA standards governing mammography and the regulations governing the release of previous mammographic studies to the facility performing the patient's current study. It seems that the standard states that these archived mammograms may be released to the facility performing the current exam WITHOUT having to have prior written/verbal consent from the patient. If this is true, how will this regulation meld with the HIPAA privacy regulations? Does anyone have any ideas/interpretations on this matter?

Answer: 1. HIPAA says a party with a valid HIPAA consent can use or disclose for treatment purposes, so provider #1 can ship to provider #2 on the authority of #1's original HIPAA consent, if it is a disclosure for treatment purposes (and if #1's notice of privacy practices doesn't promise to limit this type of disclosure - for example, by promising to require "authorizations"). In other words, post HIPAA consent, there is no barrier to sending the prior film and report if we're careful in drafting notices and consents. Specific patient "authorization" or "request" not needed if provider #1 can reasonably rely on provider #2's request as an indication the patient is going there for treatment. See p. 82519 in the preamble talking about #2's need for or use of an authorization to get records from #1:

"We expect such authorizations will rarely be necessary because we expect CEs that maintain PHI to obtain consents that permit them to make anticipated disclosures for these [treatment of the individual by another provider] purposes...."

2. The transition rules seem to say that if you have obtained pre compliance date permission (authorization, consent, etc.) to use/disclose for even ONE of treatment, payment, health care operations, then you can continue to disclose per that permission for ANY of treatment, payment or health care operations. This would probably work here as well, and is relevant because you probably won't have a HIPAA consent for old films. See 164.532.

3. See also the exception to HIPAA consent/authorization requirements when disclosure is mandated by law. (164.512(a)). I'm not that familiar with MQRSA, but I do note 21 C.F.R. 12(c)(4) on mammogram record keeping:

"Each facility that performs mammograms:

(ii) shall upon request, by or on behalf of, the patient, ...transfer the original mammograms and copies of the patient's reports to a medical institution, or to a physician or other health care provider of the patient, or to the patient directly." (emphasis added).

Seems to me that provider #2 is requesting on behalf of the patient at this point and that mandatory duty ("shall...transfer") kicks in. There may be other mandatory statements in MQRSA as well.

Bottom line, I don't think HIPAA currently throws up barriers to disclosing PHI in this case.

[Alex M. Clark]

Question: When discharge planning is undertaken with the destination being a nursing home for the first time, how should we handle the information that needs to be given to the potential facility? They require demographic, diagnosis, financial status, and the Mental Health ID screen information. Can we cover the disclosure of this information in our "Notice of Privacy" or is there another avenue?

Answer: 1. The consent you obtained is to use or disclose protected health information (PHI) for treatment, payment, and health care operations. No authorization is needed when provider A discloses to provider B for "treatment purposes." It is authorized (permitted) by the consent if the notice of privacy practices is inclusive enough. The rub is in trying to decide how much info can be disclosed for "treatment purposes." The proposed rules were quite clear that it was a referral, and that demographic and billing information could be disclosed. The final rule is not clear on this point and may limit disclosure to clinical information. This might not have been intended, but seems to be the most likely interpretation at this time. At any rate, I do not think authorization is required at the time A discloses protected health information to B in connection with treatment including placement for health services). On the other hand, B needs to get its own consent to use the disclosed PHI unless B has an indirect treatment relationship.

These disclosures for treatment purposes need to be described in the notice of privacy practices so that A's initial consent covers them.

This is a technical HIPAA answer. If a facility prefers to draft its notice so that its consent does not authorize disclosure to other providers in connection with discharge planning, and promise to obtain authorization instead, it can do so. However, I think it is then required under 164.506(a)(3)(i) to "document its attempt to obtain consent and the reason why consent [broad enough to permit the disclosure to B] was not obtained." Clear as mud! (Kelly Clarke, Baird Holm Law Firm, Omaha, NE)

2. We always have the patient or their legal representative sign an authorization to release information form when we start the discharge planning process. They may end up signing several authorizations before we actually find placement for our patients. We have tried to standardize the amount/type of information that is sent in these cases. If a nursing home has specific information they need then you can tailor your authorization so that the patient is of what you are sending and why. (Nancy Kinyoun, Health Information Manager, Hastings Regional, Hastings, NE)

Question: A couple of months ago, I posed a question to the ListServe forum about disclosure of a minor's medical record to a parent. After reading the proposed revisions, it appears that, as long as the state law is not violated and disclosure is made (with discretion) to the parent, no HIPAA violation exists. What does Nebraska law state about disclosure of a minor's medical record to the legal parent/guardian? Will this loosen the restrictions? Will this be a place to use restrictions?

Answer: Under Nebraska law, a minor can obtain counseling and treatment w/o parental consent, but an attempt must be made by the provider to involve the parent/guardian in the treatment/counseling. See Neb. Rev. Stat. 71-5041—Patricia Zieg, <pzieg@stinson.com>

Question: We have been told that workers' compensation information has to be maintained in separate files, which we find problematic. Should we do it? Any injury potentially affects a patient's total well-being, which is pertinent information to their primary provider, just as drug and alcohol abuse or HIV is pertinent to their total health picture. Have we been given incorrect information?

Answer: There has always been confusion about the contents of workers' compensation treatment records. The questions of segregation do not relate to the medical records a health care provider maintains, but to the information released to an employer. Most state workers' compensation laws permit sharing of records with the employer without authorization for treatment of work-related illness and injury. HIPAA Privacy rules also provide a broad exception to the authorization requirement based on state workers' comp laws.

The employer does not get open access to all medical records of the employee. When the health care provider sends the medical record for the treatment of an injury to the employer, the provider can only send the information relating to that injury. (E.G. Send the treatment records for an ankle fracture, but not the records relating to treatment of the employee's prostate cancer.) The concept is that the medical provider will have the complete records with HIV and drug/alcohol treatment information in order to provide effective treatment. The employer will have information limited to treatment of the work-related injury. This is when there must be a process for segregation, in keeping with the provisions of the Americans with Disabilities Act to prevent employment discrimination.

It can get complicated when there is a nexus between the prior medical treatment and the new injury. If there is a situation where the medical provider based treatment of the new injury on another existing medical condition, the employer may gain access to some of those records.

[Kathleen Zeitz, JD, Methodist Health System, Omaha, NE]

Question. Do I understand this correctly? The consent for TPO signed by the patient will include disclosure to a covered entity for health care operations - for example, physicians offices currently allow managed care companies to review their patient records for credentialing purposes. (*Ellen B. Jacobs, Director, Health Information Management Program, College of Saint Mary, Omaha, NE*)

Answer. Yes and no. The HIPAA consent does permit uses and disclosures for the covered entity's TPO purposes - expressly empowering disclosures to 3rd parties for these three purposes. When such disclosures are for the CE's health care operations, you will usually, by definition, also need a business associate agreement. These 3rd parties would be conducting functions on behalf of the CE and will fit the BA definition.

The harder part of your question is knowing whether a Managed Care Organization's credentialing activity (for inclusion in the MCO's network) fits the definition of the original CE's health care operations. Is this an activity performed on behalf of the CE under a BA agreement, or is it an activity performed for the MCO's purposes? If it is the original CE's healthcare operations, then yes, you would have a BA agreement with the MCO. You could furnish PHI on the strength of the original HIPAA consent. That would certainly be the case if you hired the MCO to do Quality Improvement studies of your care or a coding audit on your behalf.

However, I cannot tell if that is what you described. Maybe the test to apply is whether you intend to have a BA agreement with the MCO. Also, look at whether this might possibly fit the definition of "payment" activity of the CE under §164.501:

"activities undertaken by a covered health care provider ... to obtain ... reimbursement for the provision of health care."

I cannot tell more from your facts, but it does not sound like it's the CE's health care operations that are being performed with the PHI. *[Alex M. (Kelly) Clarke, Baird Holm, Omaha, NE]*

Question: At a hospital, will a blanket consent signed at registration be adequate to cover any active staff physician who treats the patient?

Answer: I am not sure what you mean by "blanket consent." However, if a hospital (or any other direct treatment provider) obtains a HIPAA compliant consent for use and disclosure of personal health information (PHI), it can share PHI for the purpose of treatment. Also, this does not fall under the minimum necessary provision. Indirect treatment providers do not need to obtain consent prior to sharing information for the purpose of treatment.

HIPAA Weekly Advisor

Editor's note: Questions were submitted by readers and answered by Tom Hanks, director of client services for PricewaterhouseCoopers, LLP's Health Care Practice, in Chicago.

Question: If a patient is required by social services to undergo weekly methamphetamine and alcohol screens in order to maintain custody of her children, can that information be kept in her medical records? I am assuming that these records would not be released with a regular release of records, such as to an insurance company. Does a medical provider have to maintain it separately, so that it is never released?

Answer

1. The drug screening is court ordered and most likely done at a court-ordered location/provider.
2. The release of PHI is covered by the court order and she does not need to approve and cannot disapprove its release to the court.
3. This testing location is most likely not her normal health care provider, so there would be no "mixing" of information.
4. In the event she did use the same providers for this, then yes, the information would be part of her permanent medical record and subject to release in the future should she give the approval. We cannot keep health records separate just because she has used drugs.

Health care information is all-inclusive. Just as you provide treatment for her asthma, cardiac problems, HIV/AIDS, or childbirth, you keep all medical information in the same file. She will have the right to release that information, but the health care providers have to keep it and protect it as a "package" deal. Under HIPAA she will have the right to limit

who can access that information, so she can mitigate the damage if the information is mixed. (*Richard Foster, Technical Project Manager*)

Additional Answer

1. The court order typically directs her to arrange for regular drug testing and directs her to see that the provider submits results of testing to the court. It does not direct the provider to take the test and submit the results. If the court order is violated (test results are not submitted), she is the one who violated it and will suffer the consequences.

2. The patient, therefore, does need to authorize release of the test results to the court. She can sign that authorization when she comes in for tests the first time (when she says that she is arranging for regular drug tests and asks to send the results to the court). Providers that I have represented in the past handled these situations with an authorization to release, because they need documentation that they could forward the test results on to the court. The only difference next year will be that the form will comply with HIPAA standards. (*Andrea M. Jahn, University Privacy Officer, Creighton University*)

Question: Under HIPAA, is there an alternative to de-identifying data when releasing it to a direct mailing company for our hospital newsletter?

Answer: Actually, de-identifying information will not work in this type of situation, because you will lose all the necessary information for the mailing list.

In order to de-identify data, you must remove personal identifiers (about 18 elements or more) or use a statistical algorithm to scramble PHI. The data elements include such demographic identifiers as patient name, address, birth date, telephone, and Social Security number. A direct mail company cannot send out a newsletter without having at least the patients' names and addresses.

Instead, you will need patient authorization. Mailing a hospital's newsletter is considered marketing. If protected health information (PHI) is provided to a business associate for marketing, it must be de-identified. Otherwise, patient authorization is required. The Privacy Regulations were revised to allow a first-time exemption to this process, but patients should be allowed to opt out from future mailings. You will need to obtain authorization after the first mailing.

QUESTION OF THE WEEK (HIPAA Weekly Advisor 12/10/2001)

Answered by Jon Bogen, president of HealthCIO Inc. in Duxbury, MA. If you have a question for him, write to BOH, P.O. Box 1168, Marblehead, MA 01945, or send an e-mail to HIPAA Weekly Advisor editor Brian Driscoll at bdriscoll@hcpro.com. *Shared with permission of HCPro*

Questions about use and disclosure:

Question: I am looking at a state statute (71-3410) which is part of legislation allowing for a death review team for Child Deaths under the Reduction in Morbidity and Mortality Law. Under provision of information and records; subpoenas it reads:

"Upon request the team (death review team previously defined) shall be immediately provided: (1) All information and records maintained by a provider of medical, dental, prenatal and mental health care, including medical reports, autopsy reports, and emergency and paramedic records; and (2) All information and records maintained by any state, county, or local government agency, including, but not limited to, birth and death certificates, law enforcement investigative data and reports, coroner investigative data and reports...and information and records of any social services agency that provided services to the child or the child's family. The Director of Regulation and Licensure shall have the authority to issue subpoenas to compel production of any of the records and information specified in subdivisions 1 and 2 of this section, except records and information on any child death under active investigation and shall provide such records and information to the team.

The next section of the statute goes on to define the confidentiality of any information acquired by the team and limits their publication and use.

My question is do you feel this will preempt HIPAA and allow this investigative team access to the information without having it completely de-identified by the source agency/provider? Since some infant deaths in rural areas are easily identified as to patient/family, there is concern that the information gathered for research will have to be de-identified to such a point that it may be useless.

Any opinions welcome. The state Pediatric Association is looking at infant mortality and may be reviving the State Child Death Review Team in which case, it may end up affecting many of us.

Answer: Section 164.512 of the HIPAA Privacy regulations lists uses and disclosures for which consent, an authorization, or an opportunity to agree or object is not required. Uses and disclosures required by law, including public health activities, fall in this category.

"A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death...."

This appears to cover the requirements and permit you to respond to such subpoenas.

Question: What does HIPAA say about telephoning patient information?

Answer: You should have policies and procedures in place that can reasonably establish the identity of the person to whom you disclose the information. That may involve establishing procedures to verify identity similar to those used by financial institutions when talking to customers over the phone, such as verification of Social Security number, address, zip code, mother's maiden name, or pre-assigned code words.

Question: Patient requested records be released to himself so he could apply for nursing home insurance. How do we protect our liability if the insurance company sells him a policy based on our records when he is clearly uninsurable?

Answer.

- 1) Under current NE law and eventually the federal law, you will have no choice but to release complete records to the patient. As long as your records are truthful, what liability would there be? Whether he is insurable or not is a business decision for whatever insurer he applies to, based on their own evaluation and standards. (Thomas J. Jenkins, Asst. General Counsel, Blue Cross & Blue Shield of Nebraska, Omaha, NE)
- 2) Also, your duty is to the patient, not to an unidentified insurance company that may have to make a business decision, not a medical decision, as to the patient. I think it would be very difficult, if not impossible, for an insurance company to blame a care provider for the decision. (Patricia Zieg, Stinson, Mag & Fizzell, PC, Omaha NE)

Question: Is it okay for our outsourcing agencies to give patients itemized statements? Is there any HIPAA provision that says the agencies cannot directly give the patient an itemized statement, or that they have to come into the office to pick up an itemized statement?

Answer: I am not sure who you are referring to as an "outsourcing agency", but you should include your release of information to these entities in your Privacy Notice that accompanies HIPAA consent. If your consent for treatment, payment and healthcare operations and Privacy Notice are comprehensive, these agencies should be able to perform their services and send their own statements.

Question: 1) We seem to have trouble with confidentiality and our local EMT's. My understanding is that they will not be subject to the privacy standards because they are volunteers for the community. Is this correct?

2) The three communities who bring patients to our ER have volunteer rescue squads runs presented at a meeting to discuss issues, concerns, education, etc. They want to

discuss patients they brought to our facility and critique how they handled care, how they could be improve the process, what went well, etc. Can we continue this type of peer review process with our facility's input? I would appreciate help with these issues.

Answer: No, "Volunteer" vs. "Paid Service" is a non-issue. All services MUST comply. You can treat them as TPAs if you want but they will have to meet the same HIPAA requirements. The problem would come in the providing information for your registration (from them) or for the EMT's documentation (from you). Without an agreement between your agencies for proper protection of patient information, you would not be in compliance.

As for base station reviews, these can be done without violating the HIPAA requirements. This can be accomplished by removing identifiable patient information for the review process. The review is on the care of the patient (i.e., how the pt. was found, vital signs, S.O.A.P., transport issues, etc). None of these discussions need the patients name, SS number, address etc.

Example Review

Pt. one

Rescue 1 (medics Smith and Doe) from eighth and main

36 y/o female c/o SOB and LOC 2nd to slip and fall

vs P - 122 s/r, Bp - 148/96, Resp 22, Eyes pearl at 8mm, A/O x 2 responds to pain etc, etc, etc.

Provided care: O2 6lpm via simple face mask, Insert OPA size 6, monitor airway, C-spine, backboard, IV Ringers tko, EKG, monitor, vs, tx C-2 to hospital, Meds en-route Narcan 2 mg IVP via IV line again etc, etc, etc.

Question: Why Narcan for a slip and fall?

Answer: Could have been drug related LOC causing fall

Question: Why Code 2 transport rather than Code 3?

Answer: Short transport time and patient was stable

Recommendations:

Base Doc: Narcan was good call, but next time Code 3 for A/O x 2 when no base contact established.

No HIPAA information is at risk in this process if done right. your issue would be during the original registration and medic paperwork process and the exchange of patient information for the process. (Richard Foster, Technical Project Manager, EMT1-A)

Question: I recently attended a meeting of the Society of Thoracic Surgeons. They have concerns that we might need a permit in order to enroll patients in the national database in order to be able to call the patients for 30-day follow-up. Do you have any information

on this? Would this also include release of patient information to the National MI registry?

Answer: I am not sure from the facts you listed whether this information would fall under the HIPAA public health exception. You should review the *Office of Civil Rights HIPAA Privacy Questions and Answers* issued on July 6, 2001 for a very good explanation of the exceptions. The regulations define when health care providers can make disclosures to public health information repositories authorized by law to collect information for public health purposes. Examples listed in the guidance include "reporting of disease or injury, reporting deaths and births, investigation the occurrence or cause of injury and disease, and monitoring adverse outcomes related to food, drugs, biological products, and dietary supplements.[Section 164.512(b)]

If a public health authority or other legal underlying authority does not authorize this registry, the exception to the need for authorization would not apply. The Preamble to the Privacy Regulations [Section 164.512(b), pp. 82668-82669] states that "Broadening the exemption could provide a loophole for private data collections for inappropriate purposes or uses under a 'public health' mask." There is a complete discussion of the regulator's analysis regarding the need for authorization for private entities' disease-specific registries. (Kathy Zeitz, JD, Methodist Health System)

Questions relating to fundraising/marketing:

Question: I have a question that I cannot answer - can anyone help? The privacy regulation does NOT define demographic information. The Comment section states that this "will generally include the name, address and other contact information, age, gender, and insurance status". For fundraising purposes, does that mean that we can or cannot disclose to our fundraisers the payer source of clients? Current practice is to omit Medicaid clients in fundraising efforts.

Answer: You ask what data elements are included in "demographic" data for fundraising purposes. First, you must understand the definitions of PHI and de-identification. Payor source is not considered one of the 18 individual identifiers. Information that contains any one or more of the 18 identifiers brings the information into the protected class of PHI. Identifiers are listed in Section 164.514(b), page 82818. Once you confirm that information is PHI, whether it includes payor source is irrelevant. The information is protected and must be treated as such. Because the information being provided is PHI, you need a Business Associate agreement with your fundraiser.

A bigger issue may be how the Minimum Necessary standards apply. If your fundraiser does not intend to target a payor source, records for that payor source should not be included at all. Do not provide information that is not required for the intended use.

Questions about Education and Training:

Question: My facility is looking to provide HIPAA training for all employees. Do you have any suggestions?

Answer: HIPAA requires providers to train all employees, but the amount and level of training needed to comply with the requirement is one of the gray areas, since the privacy standard does not offer any specifics.

This is best covered under the "reasonableness" test. The training must include all members of the workforce who have contact with protected health information (PHI).

Obviously, the training required of a large hospital differs from what's required of a small physician practice. In general, most covered entities have small budgets allocated for HIPAA training, so examining the most cost-effective method is of utmost importance.

In a small physician practice, reviewing the federal rules and the facility's privacy and security policies with all employees would probably suffice, assuming the policies are documented and available for review. The policies should be periodically reviewed and updated as the need arises. Facilities should document that employees have read and understand the updated policies.

For a larger health care organization with many dispersed employees, live classroom instruction may be feasible. Duke University Health System is providing training to the 364 managers who are involved with HIPAA compliant-operations and need to communicate the requirements to staff. The four-hour training classes for 30-40 students are held in a lecture-style classroom setting.

For other organizations, a blended approach of computer-based learning or other distance learning supplemented with live instruction has proven to be most effective. Distance learning can include a number of technologies including videoconferencing or videos, computer-based training (CBT) which includes e-learning, and other Web-based or CD-based training. One benefit to CBT is that it is self-paced; the learner goes over the educational material at his or her own rate. Another benefit is that it can be provided 24 hours a day, seven days a week.

As important as providing training is assessing whether employees understood the material presented - usually by giving them a quiz. After that, the material must be reiterated by supervisors during the work day. Most studies indicate that distance learning is only effective if it is reinforced in employees' work routines. Finally, facilities should document that the training was provided.

Generally, training responsibilities tend to be dealt with by the Human Resources (HR) department, but for HIPAA, the privacy officer or other centralized department responsible for HIPAA compliance may need to own the project.

Editor's note: Answered by Jon Bogen, President of HealthCIO Inc., Duxbury, MA. (www.healthcio.com)

Question: Is there a standard blurb we should use on new job descriptions about awareness and compliance with HIPAA?

Answer: It really does not have to be complicated. Just list one job duty as:

"Learn the confidentiality requirements and protect all identifiable health information in compliance with hospital policies and Federal/State law, including all provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)."

Substitute "clinic" or "company" for hospital for other covered entities. We solve this problem and place a high level of emphasis on confidentiality in our system by requiring all employees to sign a Confidentiality Acknowledgement at the time of employment. When you roll out final HIPAA training prior to implementation, it would be a good time to have every employee sign the form again.

We also use variations of this form for students, interpreters, external reviewers, etc.

Questions about the 'Notice of Privacy Practices'

Question: Do we have to display our notice of privacy practices, in its totality, throughout our organization, or can we just have it in one location where patients can pick it up?

Answer: The privacy regulations specify the content of the privacy notice, but give organizations some flexibility as far as how they disseminate the information to patients.

Organizations have to look at what would be the most effective means of communication. HHS will give further guidance to health care organizations on the content of the notice and communications with patients.

You are not going to want to take the entire notice and post it on the wall. If patients request it, you have to give them the entire notice. Calling their attention to it and making them aware of where they can get it will probably be sufficient. (Jill Callahan Dennis, JD, RHIA, principal of Health Risk Advantage, in Denver, and Kathleen Frawley, JD, MS, RHIA, president of Frawley and Associates, in Montclair, NJ.

The above questions are from The Greeley Company's (a division HCPro) December 10 audioconference, "The HIPAA Chief Privacy Officer...How to be successful in your new role." Go to <http://www.hcmarketplace.com/product.cfm?ID=12548> to order an audiocassette of the audioconference.

Question: Is it okay for our outsourcing agencies to give patients itemized statements? Is there any HIPAA provision that says the agencies cannot directly give the patient an itemized statement, or that they have to come into the office to pick up an itemized statement?

Answer: I am not sure who you are referring to as an "outsourcing agency", but you should include your release of information to these entities in your Privacy Notice that accompanies HIPAA consent. If your consent for treatment, payment and healthcare operations and Privacy Notice are comprehensive, these agencies should be able to perform their services and send their own statements.

Questions about incidental access:

Question: I am concerned about housekeeping personnel's access to medical records when cleaning is done after hours? It seems unreasonable to make a policy that the job role of housekeeping would have access to all records, but in point of fact when they're alone in an office containing medical records, that is exactly what they have. How should I handle these employees?

Answer: From our internal audit of those who have access to our facility, we are handling it from the Security standpoint since disclosure for use in TPO is not the issue of concern, but rather the incidental access to PHI. Housekeeping staff are treated the same as any other employee. They will be required to attend education and awareness training programs and will be held to the same standards as others who have a need-to-know access to PHI. They will sign the same agreement as our MD's.

This will also apply to our maintenance department staff who do not have a need to access PHI other than incidentally while, for example, replacing a light bulb in the medical records office. Therefore, if they breach patient confidentiality, they suffer the same consequences as any other employee.

Keep in mind that not only employees of the facility are bound by these rules, but also agents and contractors that have access your facility. You should require them to be educated and trained in HIPAA security awareness (Section 142.308). Although the Security regulations are not final yet, the proposed rules also require security controls for

PHI. More training on removing medical records from desks and other accessible sites will be necessary. *William P. Bolte, MT(ASCP) Genoa Community Hospital/LTC/PSMC*

Questions related to physical access:

Question. DOES HIPAA REQUIRE MEDICAL RECORDS TO BE UNDER LOCK AND KEY? Where should medical records be filed? We currently have locking file drawers, but they have become very cumbersome. We are planning to have open shelf units put in the office, but in order to accommodate this shelving we will have to take off the door that locks this room. Will this comply with the Health Insurance Portability and Accountability Act (HIPAA)?

Answer. Many medical record areas in various provider locations are openly accessible for legitimate staff uses to facilitate patient care. While locking file cabinets represents a secure environment for records, it is not necessary. In fact, it can be detrimental. Imagine the impact on patient care if on a given day the keys are lost or misplaced!

It is important to designate a secure area for files. While open shelving is acceptable, it must be in an area inaccessible to the public at large and to employees who should not have access to the information. If taking the lock off the door of the medical records room makes these records accessible to individuals who should not have access to the records, this decision needs to be reconsidered. It is also important to develop and maintain a system to track the location of all records, including a determination of who has accessed individual records. A periodic inventory of the records is essential to verify that your security measures are effective.

Under HIPAA providers are responsible for protecting the privacy of protected health information. It is inevitable that this will mean some changes in current policies and procedures, and perhaps some reengineering of facility and workflow design. The one caveat to keep in perspective is that HIPAA is not designed to inhibit clinical care. Decisions made to comply with HIPAA must be offset by the need to maintain expeditious patient care flow. Thus, while there is a need to protect medical records, there is also a need to allow full and unrestricted access of protected health information to those involved in the clinical treatment of the patient.

This question was answered by Joe Piccolo, CHC, compliance officer for Fox Chase Cancer Center in Philadelphia. (<http://www.fccc.edu/>) Compliance Monitor Q & A, 11/23/01

Question: PHYSICIAN USE OF PALM PILOTS Increasingly our physicians are using their personal digital assistants (PDAs) to download patient records to take home or work on after hours. Should I be concerned about these practices from a HIPAA perspective?

Answer: As more and more health care providers use PDAs or handheld computers to store their appointments, patient information, and prescription data, the likelihood of security threats increases. Many providers "synch-up" their PDAs with their appointment schedule and may download information from home to a central server. PDAs are notoriously insecure as few of them have any built-in security features.

If you have providers using PDAs to store protected health information, you need to add password authentication at a minimum. In addition, a number of technology vendors are providing PDA add-ons, which provide stronger authentication such as digital signature or fingerprint recognition. In the meantime, I recommend the following procedures for securing handhelds:

- Apply encryption to handhelds.

- Use secure sockets layer (SSL) encryption for data transported over the Internet

- Require an automatic screen saver for handhelds.

- Develop a policy on the use of handhelds to store patient data.